Designing laws to promote openness and transparency in the handling of personal data: The obligation of organisations to notify affected individuals of data breaches

ABSTRACT

Background

As organisations seek to enhance openness and access to knowledge, it becomes increasingly important to ensure that corporations who collect and store personal information relating to individuals notify the affected parties in the event of a data breach. In 2017, Australia amended its privacy laws to require designated organisations to notify the Office of the Australian Information Commissioner and affected individuals of data breaches that are likely to cause serious harm. As European law and policy makers build upon the success of the *General Data Protection Regulation* (EU) 2016/679 (GDPR) which came into force on 25 May 2018 and design laws to promote further openness in the handling of personal data in the European Union, the Australian law reform experience can provide some valuable insights into the potential operation and effect of the new data breach notification provisions of the GDPR.

Research objective

The objective of this paper is to consider the proper public policy basis for data breach notification laws, analyse the ambit of operation of such laws, and assess the merits of such law in enhancing openness and transparency in the processing of personal data. Whilst this issue has been the subject of extensive journalist discussion, it has been the subject of limited

scholarly discourse. Leading scholarship on the topic is provided by Smyth, S., and J. K. Winn[1], Wu[2], Pavolotsky,[3] Needles,[4] Garcia,[5] and Burdon[6] who examine various facets of the issue. International data surveys by PwC[7] and Protiviti Inc[8] compliment the academic literature. These works do not however incorporate the impact of the 2018 European Union *General Data Protection Regulation*. The paper will hence update the scholarly discourse and conclude by identifying continuing areas of continuing concern and suggest initiatives to further strengthen the data privacy of individuals.

Methodology

The research adopts a combined doctrinal, comparative and normative methodology as both primary and secondary legal sources (legislation, case law, governmental reports and academic literature) in Europe, the US and Australia are examined for the purpose of examining the effectiveness of the present regulatory framework and recommending options for the reform and refinement.

Keywords: Privacy; Personal data; Data security; European Union's 2018 General Data Protection Regulation.

---

[1] Smyth, S., and J. K. Winn. 2009. "Are Better Security Breach Notification Laws Possible?" *Berkley Technology Law Journal* 24 (3): 1133.
[2] Wu, X. 2014. "Data Mining with big Data." *IEEE Transactions on Knowledge and Data Engineering* 26 (1): 27–29.
[3] Pavolotsky, P. 2013. "Privacy in the Age of Big Data." *The Business Lawyer* 69: 217
[4] Needles, S. 2010. "The Data Game: Learning to Love the State-based Approach to Data Breach Notification Law." *North Carolina Law Review* 88: 267.
[5] Garcia, F. 2007. "Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time." *Fordham Intellectual Property Media and Entertainment Law Journal* 17: 693
[6] Burdon, M., J. Reid, and R. Low. 2010. "Encryption Safe Harbours and Data Breach Notification Laws." *Computer Law & Security Review* 26 (5): 520.
[7] PwC, Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016.
[8] Protiviti Inc. 2015. IT Security and Privacy Survey. The Battle Continues: Working to Bridge the Data Security Chasm, September 2015.